EMV® Chip Cards

FAQ

Frequently Asked Questions

Table of Contents

General Background 1

Geneal FAQ 2–5

Merchant FAQ 6

Processor/ATM Processor FAQ. 7

Issuer FAQ 7

U.S.-Specific FAQ 8–9

General Background

The American Express network was an early adopter of EMV® technology. In 1996, the company invested in EMV contact deployment (e.g., Chip & PIN). Today, the American Express network is EMV-enabled globally and processes millions of EMV transactions annually.

American Express is one of the key payment brands that are equity members in EMVCo, and is committed to helping secure and interoperable payments globally for chip card transactions. American Express is aligning its EMV specifications alongside other industry participants to deliver process efficiencies for all Merchants, Processors, and Issuers of American Express-branded cards.

General FAQ

1 What is EMV?

EMV is an open-standard set of payment industry specifications for integrated-circuit, chip-based payment and acceptance devices, including Point of Sales (POS) terminals and ATMs. The EMV specifications were developed to define a set of requirements to ensure interoperability between chip-based payment products and terminals.

EMV chip products contain embedded microprocessors that provide strong transaction security features and other application capabilities that are not possible with traditional magnetic stripe cards. EMVCo maintains and enhances the EMV specifications and provides product approval for terminals and chip product security on behalf of the payments industry.

2 Who is EMVCo, LLC?

EMVCo, LLC, a company owned by American Express, Discover, JCB, MasterCard, Visa and UnionPay, maintains and enhances the EMV Integrated Circuit Card Specifications to ensure global interoperability of chip-based payment cards and acceptance devices, including point-of-sale terminals and ATMs.

EMVCo also administers a testing and approval process and oversees the procedures for confirming compliance with EMV specifications. These activities include compliance testing for both chip-based POS terminals/payment accepting devices and payment cards for both the Common Core Definitions (CCD) and Common Payment Application (CPA) specifications.

Security and interoperability are the overarching goals of the EMV specifications and EMVCo. American Express, Discover, JCB, MasterCard, Visa and UnionPay have representatives in the EMVCo organization at both management and working group levels.

3 What is the status of EMV globally?

For the latest EMV statistics, visit https://www.emvco.com/about/deployment-statistics/

4 How does EMV work?

EMV cards store payment information on a secure chip rather than on a magnetic stripe. In a contact EMV transaction, the card remains in the EMV terminal throughout the transaction and exchanges information with the terminal. There are three areas of exchange that secure the transaction:

- **Card authentication:** Cards are authenticated during the payment transaction, helping protect against counterfeit cards. Transactions require card validation either online by the Issuer using a dynamic cryptogram, or offline with the terminal using Static Data Authentication (SDA), Dynamic Data Authentication (DDA), or Combined DDA with application cryptogram generation (CDA). EMV transactions also create unique transaction data so that any captured data cannot be used to execute new transactions.
- **Cardholder verification:** Cardholder verification helps ensure that the person attempting to make the transaction is the person to whom the card belongs. Cardholder verification methods (CVM) include

Offline PIN, Online PIN, and No Cardholder Verification Method for low value transactions.

- **Transaction authorization:** The transaction is authorized either online or offline. For online authorization, transaction information is sent to the Issuer, along with a transaction-specific cryptogram, and the Issuer either authorizes or declines the transaction. For offline transactions, the card and terminal communicate and use Issuer-defined risk parameters that are sent in the card to determine whether the transaction can be authorized.

5 What are DDA, CDA and SDA and how is American Express using them?

The flow of data from an EMV card is encrypted to prevent it from being intercepted or manipulated in transit by unauthorized parties. There are three data authentication methods currently employed, each with differing levels of security.

- **Static Data Authentication (SDA):** Verifies that the EMV card's contents match its digital signature. SDA will identify fraudulent cards that have invalid numbers within its digital signature. SDA cannot identify counterfeit cards that have copied all of the original card data.
- **Dynamic Data Authentication (DDA):** Verifies the EMV card's contents and detects if the card has been copied or counterfeited. DDA improves upon SDA by making use of dynamic card and terminal data elements to validate a unique cryptogram generated for each transaction by the card. This authentication method is more secure than SDA. American Express released a network mandate by which all new EMV card Issuers must use DDA technology.
- **Combined Dynamic Data Authentication (CDA):** Similar to DDA, except that the terminal performs offline data authentication while producing the application cryptogram. This combines the two processes and therefore delivers a higher level of security than is required of most applications.

6 Will contact EMV help reduce fraud and chargebacks?

Contact EMV chip-based payments have been proven to reduce fraud from counterfeit, lost or stolen cards and potentially the number of chargebacks.

Similar to other chip-based payments, the dynamic chip data generated by EMV chip-based contact and contactless transactions provide both cardholders and Merchants with enhanced security at the point-of-sale.

Secure EMV cards that perform dynamic data authentication have proven effective in combating counterfeit fraud that occurs on magnetic stripe cards. EMV cards that have been enabled with a PIN provide added cardholder verification protection against fraud resulting from a lost or stolen card.

The American Express network is EMV-enabled globally and processes millions of EMV transactions annually. Internationally, American Express has fraud liability shift rules and other chargeback-related policies that protect Merchants who have implemented EMV technology.

7 If EMV cards are more secure, why don't all cards have chips in them?

The move to EMV cards has evolved at a different pace throughout the world and requires investment in technology by both the Issuer and Merchant. While magnetic stripe cards are secure, EMV is a global standard that introduces more security features and will enable the future evolution of the global payment industry.

8 What types of Cardholder Verification Methods (CVMs) does American Express support?

The American Express Global Network specifications support all EMV recognized methods of cardholder verification, including Offline PIN, Online PIN, Signature (if applicable) and No CVM for low dollar amounts, regardless of the Issuer's EMV product presented by the Card Member at the point-of-sale. The cardholder verification method that is used at the point-of-sale will depend on the card product, terminal capabilities and transaction value.

9 What is the difference between Chip & PIN and Chip & Signature?

Chip & Signature and Chip & PIN are based on the same EMV chip-based technology. The difference is in the Cardholder Verification Method (CVM). For Chip & Signature, the Card Member signature is the verification method. For Chip & PIN, a PIN is the verification method. Chip & PIN and Chip & Signature both offer enhanced security against counterfeiting compared to traditional magnetic strip-only cards.

The Issuer decides whether to issue the card as Chip & Signature or Chip & PIN. The American Express network supports both. The Merchant terminal will indicate whether it is Chip & Signature or Chip & PIN and the steps that should follow as a result.

American Express no longer requires the capture of signature, meaning that signature is now Merchant "optional."

10 Do Merchants or banks need to capture signature?

No, capturing Card Member signature on Card Present Transactions is optional to complete a receipt and at the discretion of the Merchant, unless required by applicable law. Please contact your local American Express representative for more information.

11 What lead to the optional signature and how are Card Members authenticated now?

The growth of digital payment options, which often involve consumers authenticating themselves by fingerprint or other biometric method, has limited the need for Card Members to sign for verification purposes. American Express has also deployed advanced machine learning algorithms that allow for more precise detection of fraud while minimizing disruption of Card Members' genuine spending.

12 What is the difference between EMV contact and contactless cards?

Contact EMV cards refer to either "Chip & PIN" or "Chip" cards. Both payment cards utilize microprocessor chips, which securely store card data. The card is inserted into a terminal reader designed for chip cards.

Contactless-enabled cards allow transactions to be initiated by tapping or waving the card in front of a contactless reader at the point of sale. The contactless payment device can be a card or another form factor, such as a bracelet, key fob or smart phone. Payment information is then sent securely using radio frequency for Card or Near Field Communication (NFC), which allows a mobile device (with a payment wallet enabled) to send the required data to the reader (payment terminal). Both contactless cards and

contactless readers contain tiny antennae that allow data communication to take place. The payment device never leaves the possession of the customer, which means there is enhanced security as the card is not taken away from the Card Member and speeds up the electronic transaction process.

13 What is the difference between magnetic stripe and EMV?

Item	Magnetic Stripe Card	EMV Card
Card Stores Data	Holds basic cardholder information, i.e., the card is purely a static storage device that is read by the terminal. The terminal performs card swipe, PIN encryption functions and where merchants elect to continue to capture signature or if required by local law then they utilize the signature capture function.	Securely holds cardholder information and additional data that is used to authenticate the transaction. The issuing bank is able to define its desired processing rules via parameters on the chip. The chip's application processes information supplied by the terminal and determines how to apply the rules for processing.
Authentication Security Methods	Uses Static Data Authentication, meaning the cards might be vulnerable to counterfeit, lost or stolen, or card-not-present fraud as magnetic stripe data can be copied.	More secure in instances where fraud may occur, such as card present fraud, as an EMV card is difficult to copy and transaction data is dynamic. EMV utilizes DDA (dynamic data authentication) and sometimes also CDA (Combined DDA / Application Cryptogram Generation). Both DDA and CDA are offline authentications that validate not only that the Chip Card data has not been modified, but that the data is being read from a genuine card. In addition, the Terminal validates that the card is genuine by requesting a cryptogram from the Chip Card, meaning each transaction is uniquely secure.
Utility	Facilitates standard payment transactions.	In the future, may also facilitate additional payment and non-payment applications (e.g., loyalty programs).
Cardholder Verification Methods	Signature (if applicable)	No CVM, Signature (if applicable), Offline PIN and Consumer Device CVM (mobile).

Merchant FAQ

14 What are the benefits of EMV for Merchants?

Deploying EMV contact chip technology for payments can help Merchants optimize their business operations by delivering:

- Potential reduction in fraud-related expenses due to fewer disputed transactions made with American Express-branded cards
- Expanded interoperability as Merchants will be able to accept EMV cards from around the globe and from other payment brands
- Increased confidence for consumers who feel more secure with their transactions
- Reduced cash handling as transactions move from cash to EMV contactless
- Reduced paper used as Merchant is not required to print receipts in all cases

15 What is the cost to migrate to EMV?

Costs associated with migration to EMV vary greatly by Merchant. Some of the variables influencing the costs include which terminals are chosen, the level of external support required, and the tasks that have to be completed to integrate EMV into the Merchant network and POS.

It is strongly recommended that Merchants include American Express EMV compliant software or terminals within their point-of-sale upgrade plans.

16 What is the certification process and requirements to move to EMV?

There are varying degrees of testing that could be required as part of certification, including EMVCo testing for payment accepting devices or American Express end-to-end certification. This testing is similar to the approach of other card brands. For more information about American Express and EMV in your region, contact your American Express representative. If you are using a third-party processor to authorize and submit card transactions, you will need to work with your processor to get more details about the certification process. If you authorize or submit card transactions directly to American Express, please contact your American Express representative.

17 If terminals can accept EMV transactions, are they also able to accept mobile or contactless transactions?

EMV terminals can accept mobile or contactless transactions depending on the POS hardware and software being used. It is the Merchant's decision whether to accept contactless and mobile transactions as part of the EMV terminal upgrade. If you do, you will need to make sure the EMV terminal upgrade includes the mobile and/or contactless capabilities and is able to support the latest American Express specifications.

18 What is Fraud Liability Shift and how does it apply to EMV?

Fraud Liability Shift (FLS) is used to encourage the adoption of fraud mitigation technologies, such as EMV. For EMV, FLS transfers liability for certain types of fraudulent transactions away from the party that has the most secure form of EMV technology. The decision to implement FLS is made by each payment brand individually, on a country-by-country basis.

Processor/ATM Processor FAQ

19 What are Processors and ATM processors required to do to support EMV?

All Processors are required to certify their infrastructure to support American Express EMV chip-based contact, contactless and mobile transactions.

20 What are the American Express certification requirements for EMV?

American Express requires EMV host certification and end-to-end certification for every terminal/reader model and/or unique configuration. For further details, please contact your American Express Representative.

21 What does an ATM owner need to do to support EMV?

To support EMV, ATM owners may need to upgrade their ATM hardware and/or software, including the deployment of contact and contactless reader hardware. The ATM owners will need to coordinate the ATM hardware and/or software upgrade with their processors to ensure EMV certification has been completed.

Issuer FAQ

22 Do Issuers need to complete any certification on the American Express Card issuance infrastructure to support EMV issuance?

Yes. Issuers should contact their American Express representative to review the engagement process and certification requirements for the Issuer's chip products.

23 How long does it generally take for card-issuing partners to complete an EMV migration?

Migrating to EMV is a complex project that will impact issuing and acquiring infrastructures as well as back-end authorization systems. As the scope of each Issuer implementation could vary, an exact estimate is difficult to provide; however, for planning purposes, an Issuer should plan for an approximate 6-9 month timeframe to complete an EMV migration.

24 Does American Express offer non-financial support to Issuers to expedite the migration to EMV cards?

Yes, American Express provides an "On Behalf Of" cryptogram validation service for EMV card transactions. This enables participants to take advantage of EMV without the costs associated with building cryptogram validation logic on the Issuer's authorization host system. For Issuers using this capability, American Express will validate the cryptogram on the Issuer's behalf and forward an incoming authorization message to the Issuer for decisioning with a flag indicating whether the cryptogram was successfully validated.

U.S.-Specific FAQ

25 What does American Express' EMV roadmap in the U.S. look like?

American Express is committed to working alongside other industry participants to encourage interoperability across the U.S. and other countries and support chip-based technology transactions.

The key policy requirement dates in the U.S. are:

- In October 2015, American Express instituted a Fraud Liability Shift (FLS) policy that transferred liability for certain types of fraudulent transactions away from the party that has the most secure form of EMV technology.
- Automated Fuel Dispensers have until October 2020, before the FLS takes effect for transactions generated from automated fuel dispensers.

26 What is the Merchant demand for EMV-enabled terminals in the U.S.?

American Express has seen an increase in Merchant requests for EMV-enabled terminals in the U.S. EMV technology offers enhanced security and the potential for reduced applicable card fraud. Merchant terminals typically require both hardware (to read the EMV contact and contactless chips), American Express certified terminal product to ensure compliance and EMV software to read and interact with the chip and process incremental chip data generated. Once Merchants load their terminals with American Express compliant software, they will be required to certify their devices with American Express, if their processor has not already done so, to confirm conformance with our requirements.

27 What does it mean for Merchants to get relief from PCI DSS reporting requirements in the U.S.?

PCI DSS reporting relief refers to the reduction in PCI validation documentation required by Merchants to be in compliance with the American Express Data Security Operating Policy (DSOP). Since October 2013, Merchants are eligible to receive reduced PCI Data Security Standard (DSS) validation reporting requirements if a minimum 75% of American Express in-person transactions are processed on Point of Sale (POS) devices certified to accept American Express EMV chip-based contact and contactless transactions.

EMV Merchants may be eligible to submit an Annual EMV Attestation (AEA), which may replace the Annual Attestation of Compliance (AOC) or Self-Assessment Questionnaire (SAQ) and Quarterly Network scans currently required for American Express DSOP validation documentation. The PCI DSS reporting relief may reduce the time spent on reporting and other associated administrative efforts.

28 What is your fraud liability shift policy in the U.S.? Is this a financial incentive for Merchants?

Effective October 2015, American Express instituted a Fraud Liability Shift (FLS) policy that transferred liability for certain types of fraudulent transactions away from the party that has the most secure form of EMV technology. Following the rollout of EMV in other countries, Merchants have seen a reduction in certain types of fraud and fraud chargebacks. It is expected that Merchants will experience similar reductions the U.S. This reduction of fraud and chargebacks can result in a beneficial return on EMV-related investments by Merchants and Issuers.

U.S. fuel Merchants will have an additional two years, **until October 2020**, before the FLS takes effect for transactions generated from Automated Fuel Dispensers.

29 What was the time table for processors to convert to EMV in the U.S. for Fraud Liability Shift (FLS)?

U.S. processors were required to be enabled to support American Express EMV chip-based contact, contactless, and mobile transactions by April 2013.

30 When did American Express issue EMV chip-based cards in the U.S.?

American Express began issuing EMV-compliant cards in the U.S. in the latter half of 2012.

31 I am a fuel Merchant in the U.S., is there any U.S. specific body I can go to for more information on our region and Merchant segment?

Yes, the US Payments Forum frequently publishes information that is relevant, e.g. a Fuel Merchant FAQ, http://www.uspaymentsforum.org/petroleum-industry-emv-faq/